Code Affaire : **1-12-AIA-1900** N° Marché ou N° Cde : **2018 – 19 31 033 000 – 00 00**

Classification : **Non Protégé**

Diffusion interne : (Diffuse aux personnes concernées au sein de sa structure)

Diffusion externe :

Rédigé par	Vérifié par	Approuvé par	Approuvé par
N. CERVERA	**O. SELLIER**	**JC. PEREZ**	
Visa NICOLAS CERVERA Signature numérique de NICOLAS CERVERA Date : 2023.02.24 10:24:31 +01'00'	Visa OLIVIER SELLIER Signature numérique de OLIVIER SELLIER Date : 2023.02.24 14:28:02 +01'00'	Visa	Visa

Justification de l'application des recommandations SSI sur la Station Vol du Système FRANC

REVISIONS

IND.	DATE	SECR.	REDACTEUR	OBJET
00	**06/10/2022**		**P. AUDIBERTI**	**Version Initiale**
01	**28/12/2022**		**N. CERVERA**	**Ajout du tableau de justification en annexe validé par AIACP/SDT/PC (JC PEREZ)**

Table des matières

ANNEXES

N°	Intitulé
1	Tableau de justifications SSI

1. Identification

Ce document constitue la justification de la conformité des logiciels de la station vol du système FRANC-E2C vis-à-vis des recommandations SSI à appliquer listées dans le document [A1].

2. Documents

2.1. DOCUMENTS APPLICABLES

Rep.	Intitulé	Référence	Indice	Date
[A1]	Matrice d'application convergée SIAé AIACP	DP072596NTE008	00	27/10/2021
[A2]	Recommandations de Configuration d'un système Gnu/linux	ANSSI-BP-028	1.2	22/02/2019

2.2. DOCUMENTS DE REFERENCE

Rep.	Intitulé	Référence	Indice	Date
[R1]	FCL Carte CPU coffret FRANC – Binaire Flash	DP072596FCL001	03	06/10/22
[R2]	FCL Firmware Carte Fusion Vidéo	DP072596FCL007	02	06/10/22

3. Terminologie et sigles utilisés

Terme	Définition
FRANC	French Recorder Analyser Numeric Computer
OS	Operating System

4. Mise en place des recommandations SSI sur la carte Fusion

Sur la base du document de l'ANSSI (Cf [A2]), les recommandations convergées comme applicables dans [A1] sont appliquées au logiciel de la carte fusion et sont justifiées dans les paragraphes suivants.

4.1. R1 (MIRE) : MINIMISATION DES SERVICES INSTALLES

La liste des services présents sur la carte s'obtient en analysant le contenu du Makefile présent dans le répertoire : 02.build/05.rootfs/02.sysapps/90.build

Ce Makefile est en charge de compiler et installer l'ensembles des services disponibles sur la carte.

L'analyse du Makefile indique la compilation et l'installation des services suivants :

Service	Ecoute réseau	Rôle/Justification
btrfsprogs	Non	Utilitaires de gestion du système de fichier (btrfs)
busybox	Non	Ensemble d'utilitaires de ligne de commande. Contient comme serveurs utilisés : démon udev
rsyslog	Oui	Serveur de Log
logrotate	Non	Gestion des fichiers de log (rotation)
dropbear	Oui	Client/serveur SSH
tzdata	Non	Gestion de l'heure (fuseaux horaire)
i2c-tools	Non	Utilitaires de gestion du bus i2c pour maintenance et diagnostic. Utilisé par la procédure de validation du logiciel.
ethtool	Non	Utilitaire de configuration réseau. Utilisé par la procédure de validation du logiciel.
mtd-utils	Non	Utilitaires accès flash mtd
parted	Non	Utilitaire pour le scan des partitions
iperf3	Sur demande	Utilitaire de test en performance du réseau, pour diagnostic
phytool	Non	Utilitaire de configuration du PHY de la liaison coaxiale
ntp	Oui	Synchronisation de l'heure système avec une heure diffusée sur le réseau

⇒ ne sont présents que les composants logiciels nécessaires au fonctionnement de l'applicatif et à sa maintenance.

4.2. R2 (MIRE) : MINIMISATION DE LA CONFIGURATION

La liste des services démarrés sur la carte s'obtient via la commande :

```
# ps
  PID USER       VSZ STAT COMMAND
    1 root      2728 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 IW<  [rcu_gp]
```

```
    4 root          0 IW<   [rcu_par_gp]
    5 root          0 IW    [kworker/0:0-eve]
    6 root          0 IW<   [kworker/0:0H-kb]
    7 root          0 IW    [kworker/u4:0-bt]
    8 root          0 IW<   [mm_percpu_wq]
    9 root          0 SW    [ksoftirqd/0]
   10 root          0 IW    [rcu_preempt]
   11 root          0 IW    [rcu_sched]
   12 root          0 IW    [rcu_bh]
   13 root          0 SW    [migration/0]
   14 root          0 SW    [cpuhp/0]
   15 root          0 SW    [cpuhp/1]
   16 root          0 SW    [migration/1]
   17 root          0 SW    [ksoftirqd/1]
   18 root          0 IW    [kworker/1:0-mm_]
   19 root          0 IW<   [kworker/1:0H-kb]
   20 root          0 SW    [kdevtmpfs]
   21 root          0 IW    [kworker/u4:1-ev]
   22 root          0 SW    [rcu_tasks_kthre]
   24 root          0 IW    [kworker/0:1-eve]
   36 root          0 IW    [kworker/1:1-eve]
   40 root          0 IW    [kworker/u4:2-bt]
  205 root          0 SW    [oom_reaper]
  206 root          0 IW<   [writeback]
  208 root          0 IW<   [crypto]
  210 root          0 IW<   [kblockd]
  239 root          0 IW<   [edac-poller]
  253 root          0 SW    [watchdogd]
  280 root          0 SW    [kswapd0]
  281 root          0 IW<   [cifsiod]
  282 root          0 IW<   [cifsoplockd]
  392 root          0 SW    [spi0]
  540 root          0 SW    [irq/48-40050000]
  563 root          0 SW    [irq/31-mmc0]
  585 root          0 IW    [kworker/0:2-eve]
  589 root          0 IW<   [kworker/0:1H-kb]
  604 root          0 IW<   [kworker/1:1H-kb]
  605 root          0 IW    [kworker/1:2-eve]
  606 root          0 IW<   [kworker/1:2H-kb]
  607 root          0 SW    [jbd2/mmcblk0p1-]
  608 root          0 IW<   [ext4-rsv-conver]
  610 root          0 SW<   [loop0]
  629 root          0 SW    [jbd2/mmcblk0p2-]
  630 root          0 IW<   [ext4-rsv-conver]
  643 root          0 IW<   [kworker/0:2H]
  649 root          0 IW<   [btrfs-worker]
  650 root          0 IW<   [kworker/u5:0-bt]
  651 root          0 IW<   [btrfs-worker-hi]
  652 root          0 IW<   [btrfs-delalloc]
  653 root          0 IW<   [btrfs-flush_del]
  654 root          0 IW<   [btrfs-cache]
  655 root          0 IW<   [btrfs-submit]
  656 root          0 IW<   [btrfs-fixup]
  657 root          0 IW<   [btrfs-endio]
  658 root          0 IW<   [btrfs-endio-met]
  659 root          0 IW<   [btrfs-endio-met]
```

```
  660 root         0 IW<   [btrfs-endio-rai]
  661 root         0 IW<   [btrfs-endio-rep]
  662 root         0 IW<   [btrfs-rmw]
  663 root         0 IW<   [btrfs-endio-wri]
  664 root         0 IW<   [btrfs-freespace]
  665 root         0 IW<   [btrfs-delayed-m]
  666 root         0 IW<   [btrfs-readahead]
  667 root         0 IW<   [btrfs-qgroup-re]
  668 root         0 IW<   [btrfs-extent-re]
  669 root         0 SW    [btrfs-cleaner]
  670 root         0 SW    [btrfs-transacti]
  678 root     28588 S     rsyslogd
  688 root      2956 S     /bin/dropbear -r /etc/config/.ssh/id_rsa -d /etc/config/.ssh/id_dss
  691 root         0 SW<   [loop1]
  701 root      5628 S     {logrotate.sh} /bin/sh /etc/config/logrotate.sh
  702 root      5628 S     {sync.sh} /bin/sh /etc/config/sync.sh
  703 root      2728 S     init
  705 root      5628 S     sleep 60
  716 root     98864 S     /opt/appliFV
  719 root         0 IW    [kworker/u4:3-ev]
  720 root         0 IW    [kworker/u4:4-bt]
  721 root         0 IW<   [kworker/u5:1]
  722 root         0 IW<   [kworker/u5:2-bt]
  838 root      3084 R     /bin/dropbear -r /etc/config/.ssh/id_rsa -d /etc/config/.ssh/id_dss
  845 root      3060 S     -sh
  862 root      5628 S     sleep 1
  863 root      2592 S<    /bin/ntpdate -b -p 2 -t 1 192.168.0.12
  865 root      5628 R     ps
#
```

⇒ ne sont présents que les composants logiciels nécessaires au fonctionnement de l'applicatif :

- Serveur syslog (rsyslogd)
- Serveur SSH (dropbear)
- Client NTP (ntpdate)
- Applicatif (appliFV)

4.3. R5 (MIRE) : PRINCIPE DE DEFENSE EN PROFONDEUR

Les 4 principes sont :

1. Authentification nécessaire avant d'effectuer des opérations, notamment quand elles sont privilégiées ;
2. Journalisation centralisée d'évènements au niveau systèmes et services ;
3. Priorité à l'usage de services qui implémentent des mécanismes de cloisonnement et/ou de séparation de privilèges ;
4. Utilisation de mécanismes de prévention d'exploitation

Justification :

1. Le système est protégé par une authentification avec mot de passe
2. Les logs sont centralisés dans /var/log
3. Environnement embarqué : pas de cloisonnement (machine virtuelle ou Docker)

4. Prévention d'exploitation : les systèmes de fichier contenant les exécutables sont en lecture seule, et ne sont pas conçus pour être montés en écriture (squashfs).

4.4. R10 (IRE) : ARCHITECTURE 32 ET 64 BITS

L'ensemble du système est compilé à partir de sources. La chaine de compilation génère du code pour une architecture 64 bits.

4.5. R14 (MIRE) : INSTALLATION DE PAQUETS REDUITE AU STRICT NECESSAIRE

Le système est généré à partir de la compilation des sources de tous les composants nécessaires (« Linux from scratch »).

Il n'y a pas d'installation de paquets.

4.6. R18 (MIRE) : ROBUSTESSE DU MOT DE PASSE ADMINISTRATEUR

Test :

Vérifier que le mot de passe permettant l'accès à la console linux avec l'utilisateur root répond aux critères :

il doit comporter des chiffres, des lettres minuscules et majuscules, des caractères spéciaux et une longueur minimale de 8 caractères.

4.7. R27 (IRE) : DESACTIVATION DES COMPTES DE SERVICES

Analyse :

Visualiser le fichier 02.build/05.rootfs/99.basis/etc/default/passwd

⇒ il ne doit contenir que 2 lignes : root et nobody

⇒ seul l'utilisateur root dispose d'un shell pour se connecter (nobody pointe sur /bin/false)

4.8. R32 (MIRE) : PROTECTION DES MOTS DE PASSE STOCKES

Analyse :

Éditer le fichier 02.build/05.rootfs/02.sysapps/04.config/busybox-1.31.1.config

⇒ la propriété « CONFIG_FEATURE_DEFAULT_PASSWD_ALGO » doit être égale à « sha256 »

4.9. R36 (IRE) : DROITS D'ACCES AUX FICHIERS DE CONTENU SENSIBLE

Justification :
Un seul utilisateur : root.
Donc pas de nécessité de restriction d'accès au fichier /etc/passwd, seul fichier pouvant être concerné.

4.10. R42 (MIRE) : SERVICES ET DEMONS RESIDENTS EN MEMOIRE

Analyse

Visualiser le fichier 02.build/05.rootfs/99.basis/etc/init.d/rcS

Analyser la liste des servies et démons lancés par ce script de démarrage.

Commande	Rôle
rsyslogd	Serveur de log
/bin/dropbear -r /etc/config/.ssh/id_rsa -d /etc/config/.ssh/id_dss	Serveur SSH

4.11. R47 (IRE) : PARTITION DEDIEE POUR LES JOURNAUX

Analyse :

Éditer le fichier 02.build/05.rootfs/99.basis/etc/init.d/rcS

⇒ vérifier que la ligne suivante est présente :

ln -s /data/log /var/log

<=> les logs sont stockés dans /data qui correspond à une partition (3ième partition) différente de celle du système (qui est en lecture seule).

5. Mise en place des recommandations SSI sur CPU du coffret FRANC

Sur la base du document de l'ANSSI (Cf [A2]), les recommandations convergées comme applicables dans [A1] sont appliquées au logiciel de la carte CPU du coffret FRANC et sont justifiées dans les paragraphes suivants.

5.1. R1 (MIRE) : MINIMISATION DES SERVICES INSTALLES

La liste des services présents sur la carte s'obtient en analysant le contenu du Makefile présent dans le répertoire : 02.build/05.rootfs/02.sysapps/90.build

Ce Makefile a la charge de compiler et installer l'ensembles des services disponibles sur la carte.

L'analyse du Makefile indique la compilation et l'installation des services suivants :

Service	Ecoute réseau	Rôle/Justification
btrfsprogs	Non	Utilitaires de gestion du système de fichier (btrfs)
busybox	Non	Ensemble d'utilitaires de ligne de commande. Contient comme serveurs utilisés : démon udev
rsyslog	Oui	Serveur de Log
logrotate	Non	Gestion des fichiers de log (rotation)
dropbear	Oui	Client/serveur SSH
e2fsprogs	Non	Utilitaires de gestion du système de fichier (extfs)
tzdata	Non	Gestion de l'heure (fuseaux horaire)
i2c-tools	Non	Utilitaires de gestion du bus i2c pour maintenance et diagnostic.
ethtool	Non	Utilitaire de configuration réseau
tcpdump	Sur demande	Utilitaire d'analyse réseau, pour diagnostic
mtd-utils	Non	Utilitaires accès flash mtd
parted	Non	Utilitaire pour le scan des partitions
iperf3	Sur demande	Utilitaire de test en performance du réseau, pour diagnostic
hdparm	Non	Utilitaire de configuration bas niveau du disque dur

Ipmitools	Non	Utilitaire IPMI pour gestion du watchdog
samrtmontools	Non	Utilitaire de diagnostic bas niveau du disque dur
samba	Oui	Gestion du partage de fichier SMB (i.e. partage Windows)
ntp	Oui	Serveur NTP

⇒ ne sont présents que les composants logiciels nécessaires au fonctionnement de l'applicatif et à sa maintenance.

5.2. R2 (MIRE) : MINIMISATION DE LA CONFIGURATION

La liste des services démarrés sur la carte s'obtient via la commande ps:

```
# ps
  PID USER       VSZ STAT COMMAND
    1 root      4088 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 IW<  [rcu_gp]
    4 root         0 IW<  [rcu_par_gp]
    5 root         0 IW   [kworker/0:0-eve]
    6 root         0 IW<  [kworker/0:0H-kb]
    7 root         0 IW   [kworker/u16:0-b]
    8 root         0 IW<  [mm_percpu_wq]
    9 root         0 SW   [rcu_tasks_kthre]
   10 root         0 SW   [ksoftirqd/0]
   11 root         0 IW   [rcu_preempt]
   12 root         0 SW   [migration/0]
   13 root         0 SW   [cpuhp/0]
   14 root         0 SW   [cpuhp/1]
   15 root         0 SW   [migration/1]
   16 root         0 SW   [ksoftirqd/1]
   17 root         0 IW   [kworker/1:0-eve]
   18 root         0 IW<  [kworker/1:0H-ev]
   19 root         0 SW   [kdevtmpfs]
   20 root         0 RW   [kworker/u16:1-e]
   24 root         0 IW   [kworker/u16:2-b]
   33 root         0 IW   [kworker/1:1-rcu]
   41 root         0 IW   [kworker/0:1-mm_]
  173 root         0 SW   [oom_reaper]
  177 root         0 IW<  [writeback]
  366 root         0 IW<  [cryptd]
  387 root         0 IW<  [kblockd]
  595 root         0 IW<  [tpm_dev_wq]
  601 root         0 IW<  [ata_sff]
  626 root         0 SW   [watchdogd]
  722 root         0 IW<  [kworker/1:1H-kb]
  723 root         0 IW<  [rpciod]
  724 root         0 IW<  [kworker/u17:0-b]
  725 root         0 IW<  [xprtiod]
  765 root         0 SW   [kswapd0]
  767 root         0 IW<  [nfsiod]
  768 root         0 IW<  [cifsiod]
  769 root         0 IW<  [smb3decryptd]
  770 root         0 IW<  [cifsfileinfoput]
```

```
  771 root          0 IW<  [cifsoplockd]
  772 root          0 IW<  [xfsalloc]
  773 root          0 IW<  [xfs_mru_cache]
  808 root          0 IW<  [acpi_thermal_pm]
  917 root          0 SW   [scsi_eh_0]
  918 root          0 IW<  [scsi_tmf_0]
  922 root          0 SW   [scsi_eh_1]
  923 root          0 IW<  [scsi_tmf_1]
  926 root          0 SW   [scsi_eh_2]
  928 root          0 IW<  [scsi_tmf_2]
  929 root          0 SW   [scsi_eh_3]
  933 root          0 IW<  [scsi_tmf_3]
  937 root          0 SW   [scsi_eh_4]
  938 root          0 IW<  [scsi_tmf_4]
  942 root          0 SW   [scsi_eh_5]
  943 root          0 IW<  [scsi_tmf_5]
  947 root          0 IW   [kworker/u16:3-e]
  962 root          0 IW   [kworker/u16:4-e]
  965 root          0 IW   [kworker/u16:5-b]
 1044 root          0 IW<  [uas]
 1088 root          0 IW<  [dm_bufio_cache]
 1099 root          0 IW   [kworker/0:2-eve]
 1100 root          0 IW   [kworker/0:3-eve]
 1101 root          0 IW   [kworker/0:4]
 1112 root          0 SW   [scsi_eh_6]
 1113 root          0 IW<  [scsi_tmf_6]
 1115 root          0 SW   [usb-storage]
 1126 root          0 IW<  [kworker/0:1H-kb]
 1137 root          0 SW<  [loop0]
 1159 root          0 SW   [jbd2/sda2-8]
 1160 root          0 IW<  [ext4-rsv-conver]
 1190 root          0 IW   [kworker/1:2-eve]
 1193 root          0 IW<  [btrfs-worker]
 1194 root          0 IW<  [btrfs-worker-hi]
 1195 root          0 IW<  [btrfs-delalloc]
 1196 root          0 IW<  [btrfs-flush_del]
 1197 root          0 IW<  [btrfs-cache]
 1198 root          0 IW<  [btrfs-fixup]
 1199 root          0 IW<  [btrfs-endio]
 1200 root          0 IW<  [btrfs-endio-met]
 1201 root          0 IW<  [btrfs-endio-met]
 1202 root          0 IW<  [btrfs-endio-rai]
 1203 root          0 IW<  [btrfs-rmw]
 1204 root          0 IW<  [btrfs-endio-wri]
 1205 root          0 IW<  [btrfs-freespace]
 1206 root          0 IW<  [btrfs-delayed-m]
 1207 root          0 IW<  [btrfs-readahead]
 1208 root          0 IW<  [btrfs-qgroup-re]
 1209 root          0 SW   [btrfs-cleaner]
 1210 root          0 SW   [btrfs-transacti]
 1217 root          0 IW<  [kworker/u17:1-b]
 1218 root          0 IW<  [kworker/u17:2-b]
 1226 root      282m S    rsyslogd
 1244 root      4228 S    /bin/dropbear -r /etc/config/.ssh/id_rsa -d /etc/config/.ssh/id_dss
 1246 root      5376 S    /bin/systemd-udevd --daemon
 1749 root         0 SW<  [loop1]
```

```
 1814 root         0 IW   [kworker/u16:6-b]
 1815 root         0 IW<  [kworker/u17:3-b]
 1819 root      4088 S    {logrotate.sh} /bin/sh /etc/config/logrotate.sh
 1820 root      4088 S    {sync.sh} /bin/sh /etc/config/sync.sh
 1821 root      4088 S    init
 1823 root      3956 S    sleep 60
 1842 root     17836 S    smbd -D -s /etc/config/samba/smb.conf --private-dir=/tmp/samba/private
 1846 root      8752 S    ntpd -c /etc/config/ntpd.conf
 1854 root     17884 S    smbd -D -s /etc/config/samba/smb.conf --private-dir=/tmp/samba/private
 1897 root      505m S    /opt/diana -I
 1958 root      4444 R    /bin/dropbear -r /etc/config/.ssh/id_rsa -d /etc/config/.ssh/id_dss
 1973 root      4088 S    -sh
 2009 root      3956 S    sleep 1
 2010 root      4088 R    ps
#
```

⇒ ne sont présents que les composants logiciels nécessaires au fonctionnement de l'applicatif :

- Serveur syslog (rsyslogd)
- Serveur SSH (dropbear)
- Gestionnaire udev (systemd-udevd)
- Serveur SAMBA (smbd)
- Serveur NTP (ntpd)
- Applicatif (diana)

5.3. R5 (MIRE) : PRINCIPE DE DEFENSE EN PROFONDEUR

Les 4 principes sont :

1. Authentification nécessaire avant d'effectuer des opérations, notamment quand elles sont privilégiées ;
2. Journalisation centralisée d'évènements au niveau systèmes et services ;
3. Priorité à l'usage de services qui implémentent des mécanismes de cloisonnement et/ou de séparation de privilèges ;
4. Utilisation de mécanismes de prévention d'exploitation

Justification :

1. Le système est protégé par une authentification avec mot de passe
2. Les logs sont centralisés dans /var/log
3. Environnement embarqué : pas de cloisonnement (machine virtuelle ou Docker)
4. Prévention d'exploitation : les systèmes de fichier contenant les exécutables sont en lecture seule, et ne sont pas conçus pour être montés en écriture (squashfs)

5.4. R10 (IRE) : ARCHITECTURE 32 ET 64 BITS

L'ensemble du système est compilé à partir de sources. La chaine de compilation génère du code pour une architecture 64 bits.

5.5. R14 (MIRE) : INSTALLATION DE PAQUETS REDUITE AU STRICT NECESSAIRE

Le système est généré à partir de la compilation des sources de tous les composants nécessaires (« Linux from scratch »).

Il n'y a pas d'installation de paquets.

5.6. R18 (MIRE) : ROBUSTESSE DU MOT DE PASSE ADMINISTRATEUR

Test :

Vérifier que le mot de passe permettant l'accès à la console linux avec l'utilisateur root répond aux critères :

il doit comporter des chiffres, des lettres minuscules et majuscules, des caractères spéciaux et une longueur minimale de 8 caractères.

5.7. R27 (IRE) : DESACTIVATION DES COMPTES DE SERVICES

Analyse :

Visualiser le fichier 02.build/05.rootfs/99.basis/etc/default/passwd

⇒ il ne doit contenir que 2 lignes : root et nobody

⇒ seul l'utilisateur root dispose d'un shell pour se connecter

5.8. R32 (MIRE) : PROTECTION DES MOTS DE PASSE STOCKES

Analyse :

Éditer le fichier 02.build/05.rootfs/02.sysapps/04.config/busybox-1.33.0.config

⇒ la propriété « CONFIG_FEATURE_DEFAULT_PASSWD_ALGO » doit être égale à « sha256 »

5.9.

5.10. R36 (IRE) : DROITS D'ACCES AUX FICHIERS DE CONTENU SENSIBLE

Justification :
Un seul utilisateur : root.
Donc pas de nécessité de restriction d'accès au fichier /etc/passwd, seul fichier pouvant être concerné.

5.11. R42 (MIRE) : SERVICES ET DEMONS RESIDENTS EN MEMOIRE

Analyse :

Visualiser le fichier 02.build/05.rootfs/99.basis/etc/init.d/rcS

Analyser la liste des services et démons lancés par ce script de démarrage.

Commande	Rôle
rsyslogd	Serveur de log
/bin/dropbear -r /etc/config/.ssh/id_rsa -d /etc/config/.ssh/id_dss	Serveur SSH
/bin/systemd-udevd --daemon	Démon de mise à jour udev

5.12. R47 (IRE) : PARTITION DEDIEE POUR LES JOURNAUX

Analyse :

Éditer le fichier 02.build/05.rootfs/99.basis/etc/init.d/rcS

⇒ vérifier que la ligne suivante est présente :

ln -s /data/log /var/log

<=> les logs sont stockés dans /data qui correspond à une partition (3ième partition) différente de celle du système (qui est en lecture seule).

Tableau de justifications SSI

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD02	SEGMENT VOL : Recommandations de configuration d'un système GNU/Linux, référencé DAT-NT-28/ANSSI/SDE/NP du 12/01/2016, avec une conformité atteinte pour niveau intermédiaire.	Conforme	
CCTP-ADD02-1	R1 - M I R E Minimisation des services installés Seuls les composants strictement nécessaires au service rendu par le système doivent être installés. Tout service (particulièrement en écoute active sur le réseau) est un élément sensible. Seuls ceux connus et requis pour le fonctionnement et la maintenance doivent être résidents. Ceux dont la présence ne peut être justifiée doivent être désactivés, désinstallés ou supprimés	Conforme	La liste des services est donnée en p5/16 et p9/16
CCTP-ADD02-2	R2 - I R E Minimisation de la configuration Les fonctionnalités configurées au niveau des services démarrés doivent être limitées au strict nécessaire	Conforme	La liste des services est donnée en p5 à 7/16 et p10 à 11/16
CCTP-ADD02-3	R5 - M I R E Principe de défense en profondeur Sous Unix et dérivés, la défense en profondeur doit reposer sur une combinaison de barrières qu'il faut garder indépendantes les unes des autres. Par exemple : – authentification nécessaire avant d'effectuer des opérations, notamment quand elles sont privilégiées ; – journalisation centralisée d'évènements au niveau systèmes et services ; – priorité à l'usage de services qui implémentent des mécanismes de cloisonnement et/ou de séparation de privilèges ; – utilisation de mécanismes de prévention d'exploitation	Conforme	La justification est donnée en p7/16 et p12/16
CCTP-ADD02-4	R10 - I R E Architecture 32 et 64 bits Lorsque la machine le supporte, préférer l'installation d'une distribution GNU/Linux en version 64 bits plutôt qu'en version 32 bits	Conforme	L'ensemble du système est compilé à partir des sources. La chaîne de compilation

			génère du code pour une architecture 64 bits (p8/16 et p12/16).
CCTP-ADD02-5	R14 - M I R E Installation de paquets réduite au strict nécessaire Le choix des paquets doit conduire à une installation aussi petite que possible, se bornant à ne sélectionner que ce qui est nécessaire au besoin.	Conforme	Le système est généré à partir de la compilation des sources de tous les composants nécessaires (« Linux from scratch ») (p8/16 et p12/16)
CCTP-ADD02-6	R18 - M I R E Robustesse du mot de passe administrateur Le mot de passe root doit être suffisamment robuste compte tenu des recommandations présentes dans la note « Recommandations de sécurité relatives aux mots de passe » disponible sur le site de l'ANSSI 8. Ce mot de passe doit être unique et identique à chaque machine.	Conforme	La justification est donnée en p8/16 et p13/16
CCTP-ADD02-7	R27 - M I R E Désactivation des comptes de services. Les comptes de service doivent être désactivés.	Conforme	La procédure est donnée en p8/16 et p13/16
CCTP-ADD02-8	R32 - M I R E Protection des mots de passe stockés Tout mot de passe doit être protégé par des mécanismes cryptographiques évitant de les exposer en clair à un attaquant récupérant leur base : – hachage du mot de passe par une fonction de hachage considérée comme sûre (SHA256, SHA-512), avec un sel et un nombre de tours assez grand (65536) ; – fonction de dérivation de clé sur le mot de passe et combinée à une fonction de hachage considérée comme sûre (selon le Référentiel Général de Sécurité 10) afin d'obtenir une empreinte valide pour un aléa donné ; – chiffrement par une clé secrète (éventuellement protégée au travers d'un HSM auquel l'application accède).	Conforme	La procédure est donnée en p8/16 et p13/16
CCTP-ADD02-9	R36 - I R E Droits d'accès aux fichiers de contenu sensible Les fichiers à contenu sensible ne doivent être lisibles que par les utilisateurs ayant le strict besoin d'en connaître.	Conforme	Un seul utilisateur donc limitation (p8/16 et p13/16)
CCTP-ADD02-10	R42 - M I R E Services et daemons résidents en mémoire Seuls les démons réseau strictement nécessaires au fonctionnement du système et du service qu'ils rendent doivent être résidents et n'être en écoute que sur les interfaces réseau adéquates. Les autres démons doivent être désactivés et autant que possible désinstallés.	Conforme	La procédure est donnée en p8/16 et p13/16